DSTO

A proposed model of interoperability and a common operating environment for C3I information systems

John Mansfield

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

A proposed model of interoperability and a common operating environment for C3I information systems

John Mansfield

Information Technology Division
Electronics and Surveillance Research Laboratory

DSTO-GD-0075

ABSTRACT

This paper discusses the principles of command and control information systems from the point of view of the timely, cost effective supply of information to the commander. It is based on the premise that if the commander requires information to make a decision and the information exists within the ADF, or within allied defence organisations, then the information should be provided to the commander. It is for the commander to define the information needed to dispel the "fog of war".

It gives a definition for interoperability in this context and describes a model for information systems interoperability. It goes on to discuss the concept of a common operating environment in terms of what it is, why is it needed, what it looks like and how it may be implemented.

DEPARTMENT OF DEFENCE

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury, South Australia 5108 Australia
Telephone: (08) 259 7053
Fax: (08) 259 5619

AR-009-471
January 1996

APPROVED FOR PUBLIC RELEASE

A proposed model of interoperability and a common operating environment for C3I information systems

Executive Summary

This paper discusses the principles of command and control information systems from the point of view of the timely, cost effective supply of information to the commander. It is based on the premise that if the commander requires information to make a decision and the information exists within the ADF, or within allied defence organisations, then the information should be provided to the commander. It is for the commander to define the information needed to dispel the "fog of war".

In this context interoperability is considered to exist when two organisations can freely interchange information in a form that is immediately useable. The paper proposes a five layer model for information systems interoperability.

Policy
Procedures
Information management
Information technology
Connectivity

It goes on to discuss the concept of a common operating environment (COE) in terms of what it is, why is it needed, what it looks like and how it may be implemented. In summary, a common operating environment is more than just interoperability. An ideal COE, wherever it was used, would provide the same "look and feel" to the user, it would have the same semantics for data, the same availability of data and the same generic applications. Some of these attributes will be modified by security and need to know; others will be modified by environment - the warrior in a foxhole will not have the same range of facilities as the Assistant Chief, Operations(ACOPS) in the ADF Command Centre.

The COE can be pictured in three layers of increasing user specificity:

Architecture - This defines the overall shape, interfaces and connectivity.
Core systems - Applications, databases, etc. that are available to everyone.
Special systems - Applications, databases, etc. that have specialised and limited interest. Typically these will be such things as air tasking, sonar signature interpretation or artillery calculations.

An ADF wide C2 information systems COE is seen as a sensible approach to maximising the ADF's operational efficiency and minimising the growing cost of information technology. The downside is that it will require a strong policy statement to ensure compliance, a change in organisational structure, control of expenditure and the establishing of a central authority charged with the constant redefinition of the COE following the monitoring of user requirements and technology. A common operating environment must constantly evolve or die.

CONTENTS

1. Introduction

A command and control system is one example of a common business unit, i.e. an organisation that depends on information for its effective operation. In the beginning the only support a commander had was the information fed to him by his physical senses plus intuition honed by experience. Then shouted orders were supplemented by runners to take orders and bring back information; these runners became more sophisticated, they rode horses and motorcycles and used radio all of which increased the immediacy. More recently the transmission of information has gained speed and capacity by the use of computers and high speed telecommunications. The essential component remains the same - information.

The difference between the ancient commander and today's commander lies in the scale and speed of hostilities. Because of the high speed of today's hostilities commanders need information faster and they need considerably more information to make an informed decision. This information rarely originates from within the headquarters and needs to be drawn from superior and subordinate headquarters and facilities. In the ideal case any required information should be available instantly and the mechanism of obtaining this information from the distant source should be transparent to the commander. In this ideal case all headquarters and facilities must interoperate as one.

This paper discusses the principles of command and control information systems from the point of view of the timely, cost effective supply of information to the commander. It is based on the premise that if the commander requires information to make a decision and the information exists within the ADF, or within allied defence organisations, then the information should be provided to the commander. It is for the commander to define the information needed to dispel the "fog of war".

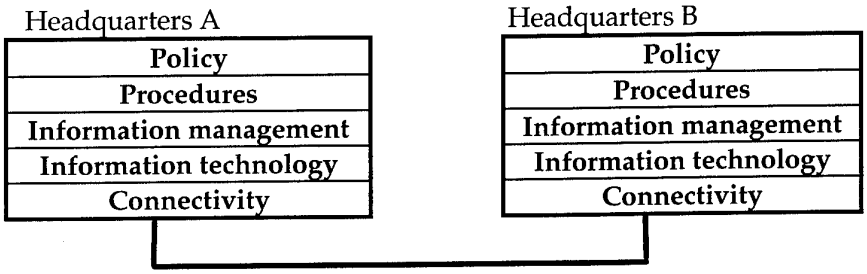
2. Interoperability

Interoperability exists when two organisations can freely interchange information in a form that is immediately useable.

Two organisations may be regarded as interoperable when they can exchange information and information based services in a timely fashion. For one organisation to exchange information with another it is not necessary that they be identical, merely that they both adopt the same mechanism for interoperating. This may be as simple as agreeing to use the telephone to exchange information but even in this simple example there are preconditions - telephone numbers need to be exchanged, times when the recipient will be within earshot of the telephone and the language to be spoken have to be arranged or assumed.

Thus interoperability only occurs when certain conditions are fulfilled, these conditions may be mandated or assumed. Interoperability is not an all encompassing entity but an attribute of two systems that is interpreted in a particular context. In the case of modern command support

systems reliant on telecommunications and computers these contexts may be grouped into a five layer model.



These layers are arranged in order of technical content but it must not be thought that any of the layers can be removed. In some cases a particular layer may play a small part because the interoperating systems are initially similar but these assumptions must still be spelled out if interoperability is not to be inadvertently lost in the future.

The meaning of the model.

Policy.

The policy layer describes the objectives of interoperability, the assumptions that are to be made and the mandated management decisions. Doctrinal changes may need to be made to take advantage of the flatter structure possible by adopting an ADF C3I common operating environment. It may be considered that the benefit to the ADF of universal interoperability is greater than the optimal efficiency of individual headquarters and facilities. Therefore, as a minimum, there must be a policy supported from the highest level that individual organisations must be designed for optimal overall interoperability even if this means that these individual organisations operate at what they perceive as less than optimal efficiency. This policy emanating from the top will need to be rigorously applied and policed as individual organisations will often see their own efficiency as more important than the ADF as a whole.

Without weakening this policy it must be recognised that the interoperability required between any two organisations in the ADF will vary depending on their function and the constraints of the technology that connects them. Complete interoperability between every organisation in the ADF is neither possible nor necessary. To illustrate this point, contrast the required and possible interaction between a strategic and an operational headquarters connected with wideband, fibre optic bearers and the required and possible interaction between a unit in the field and battalion headquarters connected with HF radio.

Procedures.

The procedures layer describes the standard operating procedures that are to be used to set up and maintain communication between organisations. Detailed procedures and the organisational structure to support procedures are more important than might at first be imagined. For example, during the five nation, combined JWID exercise, held in September 1995, Australia's ability to maintain a Common Operating Picture with the USA was hampered by the lack of procedure. Australia was interpreting OTHR Gold track messages defining the position of ships, planes, etc. using standard software however it became apparent at the start of the exercise that the USA had changed to a later, incompatible version but no one had thought to tell the Australians. There was no procedure for it.

Information management.

If data is to be used and understood ADF-wide the syntax and semantics of data will need to be defined in an ADF-wide data dictionary. The responsibility for maintaining accurate data will need to be assigned to either the generators of the data or, where that is not possible, the organisation for whom the data has the greatest importance. This responsibility for maintaining the data will not necessarily include the authority to grant or deny access to the data; this authority may be assigned to another organisation, ACOPS for example.

There are two major mechanisms for moving information between distributed, computerised ADF organisations. These are messaging and remote procedure calls. The former includes unstructured messages such as email and structured messages such as ADFORMS. The latter permits a multi-layer client server model giving applications portability, survivability and location transparency. Application level interoperability layered on top of these mechanisms is more expensive because it is achieved either by a translation mechanism or by formal, environment wide standards.

Information technology.

Information technology is the mechanism by which the information is viewed, stored and manipulated, the hardware and the software. Interoperability between different vendor's platforms and operating systems can be achieved by choosing appropriate middleware. It is not necessary to mandate a single configuration. In fact it is counter productive to mandate a single configuration because technology and, indeed, each commander's requirements are in a constant state of flux and locking in to one vendor can not provide a final solution.

Connectivity

Connectivity refers to the ability to create a link between systems. Telecommunications provides machine to machine connectivity but while this is a necessary condition for interoperability it is not sufficient; the upper layers of the interoperability model are also needed for true interoperability. The degree of connectivity will affect how well two systems can be made interoperable. Wide bandwidth fibre connections and HF radio both provide connectivity but

their initial capacity and the potential degradation of links need to be considered when deciding on the degree of interoperability.

3. A common operating environment

What is a common operating environment?
A common operating environment is a context where certain conditions have been mandated or assumed such that the required exchange of information is achieved. The five layer interoperability model may be used when defining the conditions. As a minimum, these conditions need to govern only the mechanisms for the exchange of information.

Put another way, a common operating environment provides an integrated set of information where all concerned can access whatever information they require and simultaneously know that the information is the same right across the organisation. The information can be tailored by the user to show only what they need to see; the big picture or the detail, secure in the knowledge that the underlying data has the same level of currency and integrity.

Why have a common operating environment?
Any nation that might oppose us will have access to similar weapons. Thus our command and control decision cycle must be shorter than that of our enemy so that we can use our weapons more effectively. A common operating environment is one part of that greater effectiveness. If it is such a sensible idea it might be asked why it has not been implemented before now. The answer is that the technology is only now at a point where the required level of functionality, security and connectivity is available at an acceptable cost.

The military world is characterised by a hierarchy of independent decision making. An action is repeatedly split and delegated and the process is locally optimised at each level. Initiative and independence are prized. The impact of technology has simply changed the level of communication across the hierarchy; additionally the multiplicity of complex equipment used by the modern warrior demands a multi-skilled individual. When taken together these conditions shift the emphasis to a greater availablity of information and an interchangeability of skills across and up and down the hierarchy so that information and people can be easily moved around to give the ADF a greater effectiveness. Systems originally developed in isolation for a local need are incompatible with this notion. It is therefore necessary to, as a minimum, harmonise those concepts in the five layer interoperability model which have in the past been implemented in multifarious ways through out the ADF.

It is believed that a common operating environment will provide a cost-effective and flexible capability which appears as an integrated, corporate whole, while in fact being a federation of organisations each carrying out its own tasks. It will provide direct access to information and a similarity of user interface so that multi-skilling is reduced and staff may carry out their assigned tasks efficiently, effectively and independently of location.

What does a common operating environment look like?
A common operating environment is more than just interoperability. An ideal common operating environment, where ever it was used, would provide the same "look and feel" to the user, it would have the same semantics for data, the same availability of data and the same applications. To clarify an important point, the word *application* here means generic application not a specific package. It means, for example, wordprocessing, it does not mean Word 6 or Applixware. Some of these attributes will be modified by security and need to know; others will be modified by environment - the warrior in a foxhole will not have the same range of facilities as ACOPS in the ADFCC.

The common operating environment can be pictured in three layers of increasing user specificity:

Architecture - This defines the overall shape, interfaces and connectivity of the environment.

Core systems - These are applications, databases, etc. that are available to everyone (subject to security).

Special systems - These are applications, databases, etc. that have specialised and limited interest. Typically these will be such things as air tasking, sonar signature interpretation or artillery calculations.

How do we implement a common operating environment?
A common operating environment does not need to mandate hardware or software, it can achieve interoperability by defining interfaces between systems. Once information flows are defined, current and expected mechanisms can be examined. Standards must be employed but whether these are anticipatory and de jure or de facto needs serious consideration. The lack of success of GOSIP against TCP/IP is an object lesson. However, operational and training considerations dictate a common user "look and feel" so that staff may be moved from organisation to organisation without the need for retraining. Financial considerations may also need to be taken into account when assessing bulk purchases, maintenance and software administration; but given the constant state of flux in C3I systems purchasing decisions must be taken in a short term, evolutionary manner.

The key to a workable common operating environment is flexibility. The central authority who mandates the environment should continually monitor the commercial world for new developments, evaluate them and, where they are seen as a step forward, incorporate them into the environment as quickly as possible. Some innovations, such as the Internet and the World Wide Web, appear and grow rapidly. These innovations have the potential to undermine a common operating environment if they are left unconsidered. The key is to have a policy but the policy must be flexible.

4. Conclusion

An ADF wide C2 information systems common operating environment is seen as a sensible approach to maximising the ADF's operational efficiency and minimising the growing cost of information technology. The downside is that it will require a strong policy statement to ensure compliance, a change in organisational structure, control of expenditure and the establishing of a central authority charged with its constant redefinition following the monitoring of user requirements and technology. A common operating environment must constantly evolve or die.

A proposed model of interoperability and a common operating environment for C3I information systems

J. Mansfield

(DSTO-GD-0075)

DISTRIBUTION LIST

	Number of Copies
Defence Science and Technology Organisation	
Chief Defence Scientist and members of the)	1 shared copy
DSTO Central Office Executive)	for circulation
Counsellor, Defence Science, London	(Document Control sheet)
Counsellor, Defence Science, Washington	(Document Control sheet)
Senior Defence Scientific Adviser)	1 shared copy
Scientific Adviser - POLCOM)	
Director, Aeronautical & Maritime Research Laboratory	1
Electronics and Surveillance Research Laboratory	
Chief Information Technology Division	1
Research Leader Command & Control and Intelligence Systems	1
Research Leader Command, Control and Communications	1
Research Leader Military Computing Systems Branch	1
Head, Information Management Group	1
Executive Officer, Information Technology Division	(Document Control sheet)
Head, Human Systems Integration Group	(Document Control sheet)
Head, Software Engineering Group	(Document Control sheet)
Head, Trusted Computer Systems Group	(Document Control sheet)
Head, Advanced Computer Capabilities Group	(Document Control sheet)
Head, Command Support Systems Group	1
Head, Intelligence Systems Group	(Document Control sheet)
Head, Systems Simulation and Assessment Group	(Document Control sheet)
Head, Exercise Analysis Group	(Document Control sheet)
Head, C3I Systems Engineering Group	(Document Control sheet)
Head, Computer Systems Architecture Group	(Document Control sheet)
John Mansfield, CSSG, ITD	1
Publications and Publicity Officer, ITD	1

Strategy and Intelligence

Assistant Secretary Scientific Analysis	1
Principle Research Scientist (R&D)	1
Assistant Secretary, Information Technology	1

HQADF

Director General, Force Development (JOINT)	1
Director General, Force Development (SEA)	1
Director General, Force Development (LAND)	1
Director General, Force Development (AIR)	1
Director, Operational Information Systems	1
DD-EW	1

Navy

Navy Scientific Adviser (NSA)	1

Army

Scientific Adviser, Army (SA-A)	1
Project Director, AUSTACSS	1

Air Force

Air Force Scientific Adviser (AFSA)	1

Libraries and Information Services

Defence Central Library - Technical Reports Centre	1
Manager Document Exchange Centre (MDEC) (for retention)	1
Additional copies which are to be sent through MDEC	
DIS for distribution:	
National Technical Information Centre. United States	2
Defence Research Information Centre, United Kingdom	2
Director Scientific Information Services, Canada	1
Ministry of Defence, New Zealand	1
National Library of Australia	1
Defence Science and Technology Organisation Salisbury, Research Library	2
Library Defence Signals Directorate Canberra	1
AGPS	1
British Library Document Supply Centre	1
Parliamentary Library of South Australia	1
The State Library of South Australia	1

Spares

Defence Science and Technology Organisation Salisbury, Research Library	6

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)
N/A

2. TITLE

A proposed model of interoperability and a common operating environment for C3I information systems

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document (U)
Title (U)
Abstract (U)

4. AUTHOR(S)

John Mansfield

5. CORPORATE AUTHOR

Electronics and Surveillance Research Laboratory
PO Box 1500
Salisbury SA 5108

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-GD-0075	AR-009-471	General Document	January 1996

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
N9505/10/10	ADF 93/315	DGFD (Joint)	14	N/A

13. DOWNGRADING/DELIMITING INSTRUCTIONS

N/A

14. RELEASE AUTHORITY

Chief, Information Technology Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

APPROVED FOR PUBLIC RELEASE

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE CENTRE, DIS NETWORK OFFICE, DEPT OF DEFENCE, CAMPBELL PARK OFFICES, CANBERRA ACT 2600

16. DELIBERATE ANNOUNCEMENT

No limitation

17. CASUAL ANNOUNCEMENT No limitation

18. DEFTEST DESCRIPTORS

Command and control systems
Information systems
Interoperability

19. ABSTRACT

This paper discusses the principles of command and control information systems from the point of view of the timely, cost effective supply of information to the commander. It is based on the premise that if the commander requires information to make a decision and the information exists within the ADF, or within allied defence organisations, then the information should be provided to the commander. It is for the commander to define the information needed to dispel the "fog of war".

It gives a definition for interoperability in this context and describes a model for information systems interoperability. It goes on to discuss the concept of a common operating environment in terms of what it is, why is it needed, what it looks like and how it may be implemented.